Assignment 2

CS 487/687 – CM 730
due Tuesday February 12, 5pm

February 8, 2019

Submission by email to cs487@student.cs.uwaterloo.ca

1. (8 marks) Use the power series-based algorithm to give the quotient and remainder of the division of $1 - x + x^2 - x^3 + x^4$ by $-1 - x + x^2$. You do not need to use Newton iteration for the power series inverse. Calculations done by hand or code are accepted.

In the rest of this assignment, all power series and polynomials we consider will have coefficients in $\mathbb{Q}$; all complexity estimates will count operations in $\mathbb{Q}$ at unit cost. You can reuse all results seen or used in class on the function $M$, such as

$$n \leq M(n), \quad M(n+1) = O(M(n)), \quad M(2n) = O(M(n)), \quad M(1)+M(2)+\cdots+M(2^k) = O(M(2^k)), \ldots,$$

as well as the results on the cost of power series inversion, etc.

Everybody knows that we can parametrize the circle defined by $x^2 + y^2 = 1$ by $(x = \cos(t), y = \sin(t))$ (sanity check: $\cos(t)^2 + \sin(t)^2 = 1$); $\cot(t)$ can be expanded in power series as

$$\cos(t) = 1 - \frac{1}{2}t^2 + \frac{1}{24}t^4 - \frac{1}{720}t^6 + \frac{1}{40320}t^8 + \cdots$$

It is natural to try to find parametrizations of other curves, but this is harder than it seems. In this assignment, you will look at the particular case of the curve defined by

$$y^2 = 4x^3 + 4x.$$

Weierstrass found that you can parametrize the points of this curve using a certain function $P(t) = \frac{1}{t^2} + \frac{1}{5}t^2 + \cdots$, by means of $(x = P(t), y = P'(t))$. In particular, $P'^2 = 4P^3 + 4P$. The goal in this assignment is to find the complexity of computing $n$ terms in the expansion of $P(t)$. 

1
2. (4 marks) Formula 7 on the webpage

\[\text{http://mathworld.wolfram.com/WeierstrassEllipticFunction.html}\]

gives a recurrence relation for the coefficients \(c_2, c_3, \ldots\) of \(\wp\). Using this formula, how much does it cost to get \(n\) terms? (Give a \(\Theta()\) estimate.)

3. (20 marks) First, we use Newton iteration to compute the exponential of a power series.

(a) Suppose that \(f\) is a power series of the form

\[f = f_1 t + f_2 t^2 + f_3 t^3 + \cdots,\]

with coefficients in \(\mathbb{Q}\). Prove that the coefficients of \(t^0, t^1, \ldots, t^{k-1}\) in \(f^k\) are zero.

(b) Use the previous question to prove that

\[i(f) = 1 - f + f^2 + \cdots + (-1)^n f^n + \cdots\]
\[\ell(f) = f - \frac{f^2}{2} + \frac{f^3}{3} + \cdots + (-1)^{n-1} \frac{f^n}{n} + \cdots\]
\[\exp(f) = 1 + f + \frac{f^2}{2!} + \frac{f^3}{3!} + \cdots + \frac{f^n}{n!} + \cdots,\]

are well-defined power series, with coefficients in \(\mathbb{Q}\).

You should imagine that \(\exp(f)\) is the exponential of \(f\) and that \(\ell(f)\) is the logarithm of \(1 + f\). The goal of this problem is to compute \(n\) terms of \(\exp(f)\) efficiently; we will first show how to compute \(n\) terms of \(\ell(f)\).

(c) Prove that \(i(f) = 1/(1+f)\), by proving that \((1+f)i(f) = 1\). How many operations does it take to compute \(n\) terms of \(i(f)\)?

(d) Let \(f'\) be the derivative of \(f\) with respect to \(t\). Prove that the derivative of \(\ell(f)\) with respect to \(t\) is \(f'i(f)\). Deduce that you can compute \(n\) terms of \(\ell(f)\) in \(O(M(n))\) operations.

You can freely use term-wise differentiation without justifying it.

(e) We will admit that

\[\ell(\exp(f) - 1) = f.\]

I’m not asking for a proof; instead, verify that, for \(f = t\),

\[\ell(\exp(t) - 1) \mod t^4 = t.\]

(f) If we write \(g = \exp(f)\), then the previous equality shows that

\[\ell(g - 1) - f = 0.\]

Show that the Newton iteration for this equation is

\[g_{i+1} = g_i (1 - \ell(g_i - 1) + f) \mod t^{2i+1}.\]

You don’t have to prove correctness of the iteration. You can use the fact that the derivative of \(\ell(g - 1)\) with respect to \(g\) is \(1/g.\)
(g) Taking correctness for granted, prove that you can compute \( n \) terms of \( \exp(f) \) in \( O(M(n)) \) operations.

4. (8 marks) We can use the results of the previous question to solve linear differential equations. Let \( a, b, c \) be in \( \mathbb{Q}[t] \), with \( a(0) \neq 0 \), and let \( \alpha \) be in \( \mathbb{Q} \). We want to compute the first \( n \) terms of \( f \in \mathbb{Q}[t] \) such that

\[
af' + bf = c \quad \text{and} \quad f(0) = \alpha;
\]

here, \( f' \) is the derivative of \( f \) with respect to \( t \) (termwise differentiation). Let \( B = b/a \) and \( C = c/a \). Then, we define \( J = \exp(\int B) \) and

\[
f = \frac{1}{J} \left( \alpha + \int C J \right).
\]

Here, the integrals are taken with constant term equal to zero:

\[
\int (u_0 + u_1 t + u_2 t^2 + \cdots) = u_0 t + \frac{1}{2} u_1 t^2 + \frac{1}{3} u_3 t^3 + \cdots
\]

(a) Prove that \( f \) verifies the differential equation \( af' + bf = c \), as well as \( f \mod t = \alpha \). For this, you can assume that the rules of calculus such as \( \exp(g)' = g' \exp(g) \) hold for power series (they do).

(b) Using the previous problem, show that \( f \mod t^n \) can be computed in time \( O(M(n)) \).

In the next problem, you will have to use the following fact: instead of assuming that \( af' + bf - c = 0 \), assume only \( (af' + bf - c) \mod t^{n-1} = 0 \); then you can find \( f \mod t^n \) (note the shift by 1 in the exponent) in time \( O(M(n)) \). I am not asking you to prove this.

5. (15 marks) Even better, we can solve non-linear differential equations; this leads us back to the \( \Psi \) function. The fact that \( \Psi \) starts with a term \( 1/t^2 \) is annoying. Instead, we work with \( Q(t) := 1/\sqrt{\Psi(t)} \). This is a nice power series, that starts with \( Q(t) = t + \cdots \). We will compute terms of \( Q \) instead; the terms of \( \Psi \) would be easy to recover from that.

(a) Prove that \( Q \) satisfies

\[
Q^2 = 1 + Q^4.
\]

Suppose that we know \( Q \mod t^s \), for some \( s \geq 2 \). We write \( Q = Q_0 + Q_1 \), where \( Q_0 = Q \mod t^s \) is known and \( Q_1 \) is unknown. What we know by definition is that \( t^s \) divides \( Q_1 \).

(b) Prove that \( t^{s-1} \) divides \( Q_1 \).
(c) Prove that $t^{2s-2}$ divides $Q_1^2$, $Q_1^2$, $Q_1^3$ and $Q_1^4$.

(d) Rewrite Eq. (1) in terms of $Q_0$ and $Q_1$ and take it modulo $t^{2s-2}$.

(e) Use the previous problem to compute $Q_1$ mod $t^{2s-1}$; this gives you $Q$ mod $t^{2s-1}$.

(f) What is the complexity of computing $Q$ mod $t^n$? (A sketch of proof is enough.)

Note: here are the successive truncations of $Q$ that you would find, with the corresponding $s$:

\[
\begin{align*}
    s = 2, & \quad Q \mod t^2 = t \\
    s = 3, & \quad Q \mod t^3 = t \\
    s = 5, & \quad Q \mod t^5 = t \\
    s = 9, & \quad Q \mod t^9 = t - \frac{1}{10}t^5 \\
    s = 17, & \quad Q \mod t^{17} = t - \frac{1}{10}t^5 + \frac{1}{120}t^9 - \frac{11}{15600}t^{13} \\
    s = 33, & \quad Q \mod t^{33} = t - \frac{1}{10}t^5 + \frac{1}{120}t^9 - \frac{11}{15600}t^{13} - \frac{211}{3536000000}t^{17} - \frac{1607}{318240000}t^{21} \\
        & \quad + \frac{1511}{3536000000}t^{25} - \frac{71985888000000}{318240000}t^{29}
\end{align*}
\]

From the last value, we deduce

\[
\mathcal{P}(t) = \frac{1}{t^2} + \frac{1}{5}t^2 + \frac{1}{75}t^6 + \frac{2}{4875}t^{10} + \frac{1}{82875}t^{14} + \frac{2}{6215625}t^{18} + \frac{2}{242409375}t^{22} + \frac{4}{19527421875}t^{26} + \ldots
\]

6. (2 marks) How much time did you spend on the assignment?